Judiciary Committee Passes Legislation to Combat Spyware

Media Contact: Heather Wong, 202.225.3072

Washington, DC -- The House Judiciary Committee today passed the "Internet Spyware (I-SPY) Prevention Act of 2005, H.R. 744, which was introduced by Representatives Bob Goodlatte (R-VA-06), Zoe Lofgren (D-CA-16) and Lamar Smith (R-TX-21). This bipartisan legislation, which passed the House of Representatives last Congress by a vote of 415-0, addresses the most egregious activities that are conducted via spyware and makes those activities criminal offenses.

Spyware has been defined as "software that aids in gathering information about a person or organization without their knowledge and which may send such information to another entity without the consumer's consent, or asserts control over a computer without the consumer's knowledge." In April 2004, the Federal Trade Commission testified before a House Subcommittee that "spyware appears to be a new and rapidly growing practice that poses a risk of serious harm to consumers".

"I am encouraged by the passage of this legislation through the Judiciary Committee," said Rep. Bob Goodlatte. "I believe that four overarching principles should guide the development of any spyware legislation. First, we must punish the bad actors, while protecting legitimate online companies. Second, we must not over-regulate, but rather encourage innovative new services and the growth of the Internet. Third, we must not stifle the free market. Fourth, we must target the behavior, not the technology. The I-SPY Prevention Act is a targeted approach that protects consumers by imposing stiff penalties on the truly bad actors, while protecting the ability of legitimate companies to develop new and exciting products and services online for consumers."

The legislation would make the following criminal offenses:

Intentionally accessing a computer without authorization, or intentionally exceeding authorized access, by causing a computer program or code to be copied onto the computer and using that program or code to

-Further another federal criminal offense (punishable by fine or imprisonment for up to 5 years)

-Intentionally obtain or transmit "personal information" with the intent of injuring or defrauding a person or damaging a computer (punishable by fine or imprisonment for up to 2 years)

-Intentionally impair the security protections of a computer (punishable by fine or imprisonment for up to 2 years)

The legislation includes language to preempt States from creating civil remedies based on violations of this act.

The legislation also authorizes $10 million to the Department of Justice to combat spyware and phishing scams. "Phishing" scams typically involve the use of fake e-mail messages and websites to lure consumers into providing bank account information, credit card numbers and other personal information. These fake e-mail messages and websites are often indistinguishable from the real ones and often request account information from consumers.

"Spyware makes spam look like child's play and is one of the key reasons why we have an identity theft epidemic in this country," said Rep. Zoe Lofgren. "The I-SPY Prevention Act is unique because it focuses on behavior, not technology, and it targets the worst forms of spyware without unduly burdening technological innovation. I believe that this legislation will help stem the spyware tide and contribute to a solution that protects businesses and consumers without slowing innovation."

Spyware encompasses several potential risks including the promotion of identity theft, by harvesting personal information from consumers' computers. Additionally, it can adversely affect businesses, as they are forced to sustain costs to block and remove spyware from employees' computers, not to mention the potential impact on productivity.

"Computer spyware is a growing problem that threatens personal privacy and the future of commerce over the Internet. Each day, thousands of unsuspecting Americans have their identities hijacked through spyware programs. Victims of this crime can spend years trying to restore their good name and credit," said Rep. Lamar Smith. "Passage of this bill will ensure that those who engage in this type of criminal behavior are punished accordingly."

There is also a growing concern that persistent computer security vulnerabilities may expose U.S. critical infrastructure and government computer systems to cyber attacks, which would ultimately jeopardize national security and the economy.

"The Center for Democracy and Technology has seen several egregious examples of spyware being used in ways that most Americans would think clearly ought to be criminal. The Goodlatte, Lofgren, and Smith bill will help make sure that there are strong deterrents to using spyware to defraud or injure consumers," said Ari Schwartz, Associate Director of the

Center for Democracy and Technology, part of a broad coalition of consumer groups addressing the spyware problem.